Solovay Contents

Peter Gács

I Randomness properties of $\Omega = \sum_n M(n)$.

Relation of various definitions of randomness.

<u>Def</u> t a <u>weak test</u> if

$$\lim_{m \to \infty} \mu\{x : t(x|\mu) > m\} = 0 .$$

<u>Theorem</u>

Each r.e. real fails under some weak test.

II. $H(H(x)|x)$.

<u>Conjecture</u> $\forall n \exists x \in {}^n 2 \quad H(x) \approx n , \quad H(H(x)|x) \approx \log n$

(In our examples we may have $H(x) < n / \log\log n$)

Why not $n/\log n$?

III. Various formulas relating H and K.

Can be approximately summarized in

$$H(x) \asymp K(x \mid H^2(x)) + H^2(x)$$

where $H^2(x) = H(H(x))$.

IV. The relation of the tests

$m_H(x) = |x| - H(x)$ and $m_K(x) = |x| - K(x)$.

It is shown that

$$m_H \gtrsim m_K + O(\log m_K)$$

$$m_K(x) \gtrsim m_H(x) + O(\log_2 |x|),$$

and this is sharp.

V. Upper bounds on H that are sharp infinitely often.

(See my dissertation for a shorter construction)

More: $\exists h$

$$\overline{\lim} \frac{1}{n} \# \{ m : m \leq n \ \& \ h(m) = H(m) \} > 0 .$$

$\forall h \qquad \underline{\lim} = 0$,

moreover: no rec. seq. D_n with

$m \in D_n \rightarrow m \geq n$ & $\exists x \in D_n \quad h(x) \leq H(x) + C$.

VI On $s(m)$, $\alpha(m)$,

$D_n = \{x : l(x) \le n$ & $U(x)$ is defined$\}$, and Ω_n, and the sets $\{x : H(x) = m\}$. Here $s(m) = -\log\left(\sum_{n>m} M(n)\right)$, $\alpha(m) = \min_{n \ge m} H(n)$.

I think I can prove that

$$\alpha(m) \lesssim s(m) + H(s(m))$$

cannot be substantially improved.

$\log \# D_n \asymp n - H(n)$, as well as the cardinality of some related sets.

$$H(D_n) \asymp n \quad , \quad H(D_n \mid \Omega_n) \asymp 0 \asymp H(\Omega_n \mid D_{n+H(n)})$$

VII. On $H(\Omega_n)$.

Let g_0 be recursive, $\sum_j 2^{-g_0(j)} = \infty$,

g_1 be rec. mon. such that $g_1 \to \infty$.

Let x be random. $\exists_\infty n$

1) $H(n) \ge g_0(n)$ and

either 2a) $H(x^n) \ge n + g_0(n)$

or 2b) $H(x^n) \le n + g_1(n)$ (analogous to Martin-Löf's oscill. result)

$H(x^n) - n \to \infty$ for random x, because $\sum 2^{n - H(x^n)}$

is a test. This result may make some proofs [illegible] [illegible]

To the proof of 2b: let $A_n \subset {}^n2$, $\sum \mu(A_n) = \infty$,
$g_2(n) = -\log \mu(A_n)$, $\bigcap_m \bigcup_{n \geq m} A_n$ = the whole space

Then $$\sum M(n) \cdot \frac{\mu_{A_n}(x)}{\mu(A_n)} \lesssim M(x)$$

for $x \in A_n$, $H(x) \lesssim -\log \mu(x) + H(n) + g_2(n)$
Now for g_1 let g_2 be such that $\sum 2^{-g_2} = \infty$, $\sum 2^{-(g_1+g_2)} <$
Then $H(x) \lesssim -\log \mu(x) + g_1(n)$, for all x,
$H(n) \gtrsim H(x) + \log \mu(x) + g_2(n) \gtrsim g_2(n)$ for random x.

Def. Ω-like r.e. real: $\exists F, C \; \forall q < \Omega \quad |\Omega - F(q)| \leq C(\Omega - q)$
Note: α is Ω-like iff $H(\alpha^n) \asymp H(\Omega_n)$.

VII A. Ω and the arithm. random reals.

~~$K(\Omega_n)$~~ $\leq$

1) If x is arithm. random then $\exists C \, \exists^\infty n$
$$H(x^n) \geq n + H(n) - C$$

2) $H(\Omega_n) \leq n + H(n) - \alpha(n) + \overbrace{O(\log \alpha(n))}^{\leq c}$

~~Hence (Bales) K(Ωₙ) ≤~~ Similarly, $K(\Omega_n) \leq n - \alpha(n) + O(\log \alpha(n))$.

3) If x is arithm. random then
$$H(x^n) \geq n + \alpha(n) + O(\log \alpha(n))$$

4) $\exists^\infty n \quad H(\Omega_n) \leq n + \alpha'(n) + O(\log \alpha'(n))$.

For 1): the function $\sup_m \inf_{n \geq m} n + H(n) - H(x^n)$

is an arithm. test.

2). Knowing n we know a little segment of Ω.

3) $M(x^n|\nu) \gtrsim M([S(n)]) \cdot M(x^n) \cdot 2^{S(n)}$,

$n - H(x^n|\nu)$ is an arithm. test.

4) Using a segment of Ω to compute a length.

VIII. Non-recursive sets with $H(x^n) \asymp H(n)$.

Notes to Solovay's Chapter $\overline{\text{VIII}}$. (Peter Gacs)

The only thing we want to replace is Lemma $\overline{\text{VIII}}$.3.

Let $\Phi_e(x)$ always measure the storage requirement of the computation of $\{e\}(x)$.

We assert that the priority construction will work with $t_i = 6^i$. To see this, we prove a lemma replacing Lemma $\overline{\text{VIII}}$.3. Let

$$H(x\,;t) = \min\{|p| : U(|p|) = x \ \& \ \Phi(p) \le t\}.$$

$$M(x\,;t) = \exp(-H(x\,;t))$$

$$s(n\,;t) = -\log\Big(\sum_{i \ge n} M(x\,;t)\Big)$$

$$m(k\,;t) = \min\{n : s(n\,;t) > k\}$$

Note that $m(k\,;t) \nearrow m(k\,;\infty) < \infty$.

Lemma $\overline{\text{VIII}}$.3' We have for all k and $n \ge m(k,t)$

$$H(n\,;t) - H(n\,;6t) \gtrsim k - H(k,t\,;6t)$$

Proof of Lemma $\overline{\text{VIII}}.3'$ Let $n \geq m(k,t)$.

We give a program of length

$$H(k,t;6t) + H(n;t) - k$$

computing n within space $6t$.

Let p be a program computing (k,t) within space t. We set off, with the help of p, six ~~store~~ areas of length $S_0, \dots, S_5$. We store $\ulcorner t \urcorner$, $\ulcorner k \urcorner$ and a piece of program q of length $H(n;t) - k$ to be specified later in areas S_0 and S_1.
Let x_i be an enumeration of the words of length $\leq t$.
S_2 will keep track of x_i.
S_3 will keep track of the numbers r with $\log r \leq t$.
S_4 will keep track of $\Sigma\{2^{-|x_j|} : j < i,\ \varphi(x_j) \leq t,\ U(x_j) \geq r\ \}$
S_5 is reserved for the actual computations.

After computing and storing t and k, we proceed to compute $m(k,t)$. For each r with $\log r \leq t$ we compute $\lfloor s(r;t) \rfloor$ by accumulating the sum mentioned above in S_4.

We stop when $|s(r;t)| \le k$: then we arrived at $r = m(k;t)$

Now we again begin accumulating, in S_4, the sum

$$a_i = \sum \{ 2^{-|x_j|+k} : j < i, \ \Phi(x_j) \le t, \ U(x_j) \ge m(k,t) \}.$$

Let $U(x_i) = n$, $\Phi(x_i) \le t$, $|x_i| = H(n;t)$. We have

$a_{i+1} - a_i = M(n;t)$, hence if q localizes the interval

(a_i, a_{i+1}), we will be able to recover n. Q.E.D.

Application of Lemma VIII.3'

We must show that with this t_n, and the $\sigma(n)$ defined in Solovay VIII, for any recursive function $\{e\}(x)$ we have infinitely often $\Phi_e(\sigma(n)) \le n$.

Proof Let i_k be the least i with the following

property: For all $j \le m(k, 6^i)$, $\{e\}(j) < i$.

Clearly i_k is computable from k within space $5 \cdot 6^i$, since, as we have seen in the proof of Lemma VII 3', $m(k, 6^i)$ is. Thus $H(k, 6^{i_k}; 6^{i_k+1}) \leq 2 \log k$,

and for $n \geq m(k, 6^{i_k})$,

$$H(n; 6^{i_k}) - H(n; 6^{i_k+1}) \geq k - 2 \log k > 1 .$$

Hence

$$\sigma(i_k) < m(k, 6^{i_k}),$$

i.e. $\varphi_e(\sigma(i_k)) \leq i_k$.

Q.E.D.

I. Randomness properties of Ω.

Recall that the real Ω is defined as the sum

$$\sum \{2^{-|p|} : U(p) \text{ is defined}\}.$$

(Chaitin uses lower case ω, but we use that as our notation fo

Here U is the universal Chaitin computer and the non-negative int

$|p|$ is the length of the program p.

It is clear that ω is an r.e real in the sense of the following definition.

<u>Definition 1</u> A real x is r.e. if there is a recursive sequence of rationals $\langle x_n, n \in \omega \rangle$ which is weakly monotone (i.e, $n \leq m \rightarrow x_n \leq x_m$) and has the limit x.

Equivalently, x is r.e. if $\{q \in \mathbb{Q} : q < x\}$ is r.e

(These two definitions are, in fact, effectively equivalent, in that we can effectively go from a Gödel number for $\langle x_n \mid n \in N \rangle$ to one for $\{q \in Q : q < x\}$, and vice versa.) Note also, that we can choose the sequence x_n in Definition 1 to consist of dyadic rationals.

A randomness property of reals is a property that holds of all reals except for a set of Lebesgue measure zero. (For example, let M be a transitive model of some suitable fragment of axiomatic set theory. We say that x is random over M, if x lies in no Borel set of measure zero which can be

encoded by a real in M. (Cf. [Sol 1, Chapter II], where this notion is discussed and shown to be a randomness property.

Now obviously almost all reals are not r.e, and thus sufficiently strong randomness properties are not possessed by Ω. We are going to investigate in this chapter the following two questions.

1) What randomness properties are properties of some r.e real?

2) Which of these are properties of Ω?

Of course these questions are somewhat vague. Before stating our results precisely, we need some

preliminary definitions. We pick an effective enumeration of all open intervals with rational end-points, $\langle I_0, I_1, \ldots \rangle$. Then we say a recursive function $h: \omega \to \omega$ gives a recursive enumeration of the open set $U \subseteq \mathbb{R}$ if

$$U = \bigcup_{n\in\omega} I_{h(n)}.$$

(By definition, U is r.e. iff such an h exists.)

A sequence of open sets $\langle U_n ; n\in\omega \rangle$ is simultaneously r.e. if there is a recursive map $h: \omega^2 \to \omega$ such that

$$U_n = \bigcup_{j\in\omega} I_{h(n,j)}.$$

We now proceed to list certain properties of a real x in $[0,1]$.

$P_1(x)$: Let $\langle U_n ; n \in \omega \rangle$ be a simultaneously r.e. sequence of open sets. Suppose that the sequence $\langle U_i \mid i \in \omega \rangle$ is decreasing (i.e. $m \le n \to U_n \subseteq U_m$) and that $\mu(U_n) \to 0$. Then $x \notin \bigcap_n U_n$

$P_2(x)$; Let $\langle U_n ; n \in \omega \rangle$ be a simultaneously r.e. sequence of open sets. Suppose further that

(1) $\displaystyle\sum_{i=0}^{\infty} \mu(U_i) < \infty.$

Then $x \in U_i$ for only finitely many i.

$P_3(x)$: Similar to P_2 except we require the U_i's to satisfy the following additional requirement: There is a recursive function $h: \omega \to \omega$ such that $\displaystyle\sum_{i=h(n)}^{\infty} \mu(U_i) \le 2^{-n}.$

(I.e. we should have an effective bound on the rate of convergence in (1).)

P_3': Similar to P_1 except we require that $\mu(U_n) < 2^{-n}$.

$P_4(x)$: This says first (to avoid some trivial cases) that x is not a dyadic rational and lies in the unit. Thus the dyadic expansion of x is well-defined. Let $x(n)$ be the first n-digits of x. Then for some C,

$$H(x(n)) > n - C$$

infinitely often in n.

We shall see in a moment that $P_1(x)$ holds for almost all reals x, and that the implications

$$P_1(x) \rightarrow P_2(x) \rightarrow P_3(x) \longleftrightarrow P_3'(x) \rightarrow P_4(x)$$

are trivial.

$P_3(x)$ is the notion of Martin-Löf randomness (cf. [ ].) $P_4(x)$ is the notion of randomness proposed by Chaitin in [ ]. Schnorr has announced the theorem: $P_3(x) \longleftrightarrow P_4(x)$. Chaitin shows that $P_4(\Omega)$ in [ ]. Here are the main results of this chapter

1) $P_1(x)$ holds for no r.e real, x.

2) $P_2(\Omega)$ is true. (The results of Chaitin and Schnorr that $P_4(\Omega)$ and $P_3(\Omega)$ of course follow.)

3) $P_2(x) \longleftrightarrow P_3(x)$.

Thus $P_2(x)$ is just another way of expressing Martin-Löf randomness. Our result is a bit surprising since the obvious Borel-Cantelli variant of M.L. randomness is P_3.

I.1. Let us begin with the trivial facts recalled above. In the first place for any sequence $\langle U_i, i \in \omega \rangle$ as in P_1, $\bigcap_i U_i$ is a Borel set of measure zero. But there are only countably many ~~re~~ such simultaneously r.e. sequences of open sets, and the union over all such $\langle U_i \mid i \in \omega \rangle$, as in P_1, of the corresponding sets $\bigcap_i U_i$ has measure zero. Thus almost all reals avoid all such

sets and so satisfy P_1.

Next let x satisfy P_1. Let $\langle U_i \mid i \in \omega \rangle$ be as in P_2. Put $W_n = \bigcup_{m=n}^{\infty} U_m$. Then $\langle W_n \mid n \in \omega \rangle$ is simultaneously r.e. and $\overline{\lim}\, \mu(W_n) \leq \overline{\lim} \sum_{m=n}^{\infty} \mu(U_i) = 0$. Thus $x \notin W_n$, some n, by P_1. Thus $x \in U_i$, only for $i < n$, Thus ~~so~~ x satisfies P_2

It is utterly trivial that $P_2(x) \rightarrow P_3(x)$, and the proof that $P_3'(x) \rightarrow P_3(x)$ can be gotten along the lines of the proof that $P_1(x) \rightarrow P_2(x)$ just given.

Suppose conversely that x satisfies $P_3'(x)$.

~~We put~~

Let $\langle U_n \mid n<\omega\rangle$ be as in P_3, and let $h:\omega\to\omega$ be also as in P_3. Define $\langle W_n \mid n<\omega\rangle$ by

$$W_n = \bigcup_{m=h(n)}^{\infty} U_m.$$

Then $\mu(W_n) < 1/2^n$ & the W_n's are simultaneously r.e. By P_3', (x), $x \notin W_n$, some n. But then $x \notin U_i$, for $i \geq h(n)$, as was to be shown.

The proof that $P_3(x) \to P_4(x)$ is essentially in Chaitin. Recall that for some constant C independent of m, n,

$$\mu(\{x \in {}^n[q,2]: H(x(n)) \leq H(n)+n-k\}) \leq C\cdot 2^{-k}.$$

Thus $\mu(\{x \in 2^\omega : H(x(n)) \leq n - k\}) \leq C \cdot 2^{-H(n)-k}$

~~On the other hand,~~ $\cancel{\sum_{n=0}^{\infty} H(n) < 1.}$ ~~So~~

$$\cancel{\mu(\{x \in 2^\omega : (\exists n)(H(x(n)) \leq n-k\})}$$

$$\cancel{\leq C \cdot 2^{-k}}.$$

Let $W_k =$

$$\{x \mid (\exists n)\ H(x(n)) \leq n - k\}.$$

Then $\mu(W_k) \leq C \cdot 2^{-k} \left(\sum_{n=0}^{\infty} 2^{-H(n)}\right)$.

Also the $\langle W_k \mid k \in \omega \rangle$ are simultaneously r.e. (For the purposes of this proof, view each dyadic rational as given its non-terminating dyadic expansion. It is necessary to check that each dyadic rational lies in W_k, all k. But this is clear since if $\forall x$

is dyadic $H(x(n)) \leq H(n) + O(1) << n.$)

By a theorem of Chaitin, $\sum_{n=1}^{\infty} 2^{-H(n)} < 1$.

Thus $\mu(W_n) \leq C \cdot 2^{-n}$ & we can apply

P_3 to conclude $x \notin W_k$, some k. Whence

$$H(x(n)) \geq n - k, \text{ all } n$$

and x satisfies P_4.

I.2 We turn to the proofs of our main results of this chapter. The first is

<u>Theorem I.1</u>. Let x be an r.e. real. Then x does not satisfy P_1.

The proof we present is due to D. A. Martin, and was arrived at at about the same time as the

authors proof. We present Martin's proof since it is conceptually simpler.

Let x be an r.e. real. We ~~let x_n~~ may assume $0 \leq x \leq 1$, and let x_n be a monotone increasing recursive sequence of reals with limit x. ~~We define U_n~~ Note that if x is rational, the sequence

$$W_n = \mathbb{Q}(x - 2^{-n}, x + 2^{-n})$$

shows that x does not satisfy even P_3. So we assume x irrational.

Now define $U_n = (x_n, x_n + 2(x - x_n))$.

It is clear that the U_n's are a decreasing

sequence of open sets containing x. Moreover

$\mu(U_n) = 2|x - x_n| \longrightarrow 0$. To complete

the proof that x does not satisfy P_1, we show

that the $\langle U_i \mid i \in \omega \rangle$ are simultaneously r.e.

But this is clear since

$$U_n = \bigcup_{m>n} (x_n, x_n + 2(x_m - x_n))$$

~~Re~~ I.3. __Theorem I.2.__ Let Ω be as

in Chaitin's paper. Then Ω satisfies P_2. ? *

__Proof.__ (Again I would like to thank

D. A. Martin for making a remark which led to

the present proof.)

* Why bother if
$P_2 \Leftrightarrow P_4$ &
Chaitin proves $P_4(\Omega)$)

Let then $\langle U_n \mid n<\omega \rangle$ be a simultaneously r.e.

sequence of open sets such that ~~$\mu(U_n)$~~

$$\sum_{i=0}^{\infty} \mu(U_n) \le C < \infty.$$

By deleting a finite no. of the U_n's, we may assume $C = 1$.
For the moment, let N be any positive integer. (N will be fixed presently.) Let

$$W_N = \{ x \mid x \in U_n \text{ for } N \text{ distinct values of } n \}.$$

First, what is the measure of ~~W_n~~ W_N. If A is any set, let χ_A be its characteristic function: $\chi_A(x) = 1$ for $x \in A$, and equals 0 otherwise. Let

$$g = \sum_{n=0}^{\infty} \chi_{U_n}.$$

Then $\int g = \sum_{n=0}^{\infty} \mu(U_n) = \cancel{\le}\ 1$.

On the other hand, by the definition of W_N,

$0 \le N \chi_{W_N} \le g$

Integrating this equation we get $N \mu(W_N) \le \cancel{g}\ 1$

I.e. $\mu(W_N) \le \cancel{g/N}\ 1/N$.

Next we claim that ~~that~~ $\langle W_N \mid 1 \le N < \omega \rangle$

is simultaneously r.e. ~~Indeed~~

~~$W_N = \bigcup \{ (a,b) : a, b \in Q$ and $[a,b] \subseteq W_N$~~

~~Thus it suffices to see ??~~

~~$\{ [a,b] : a, b \in Q, a < b$ & $[a,b]$~~

Let $x \in W_N$. Then for some $n_1, \dots, n_N$

$x \in U_{n_i}$, $1 \le i \le N$. Since the U_i's are open,

there are rationals $a < x < b$: $[a,b] \subseteq U_{n_i}$,

$1 \le i \le N$. (So $[a,b] \subseteq W_N$.) It follows

that

$$W_N = \bigcup \{ (a,b) : a, b \in \mathbb{Q},\ a < b \ \&\ [a,b] \subseteq U_i,$$

for at least N i's $\}$.

Whence it suffices to see that

$\{ (a,b,i) : [a,b] \subseteq U_i \}$ is

r.e. Let $h : \omega^2 \to \omega$ be as in the definition

of simultaneously r.e. Then, by compactness of $[a,b]$

$[a,b] \subseteq U_i$ iff

$(\exists n) \left([a,b] \subseteq \bigcup_{j=0}^{n} I_{h(i,j)} \right)$.

That the expression in parentheses is recursive is

a trivial piece of combinatorics that we leave to the

reader.

We now indicate our plan to show $\Omega \in U_n$ for only finitely many n. Ω is defined in terms of the universal Chaitin computer, U. U must in term simulate all other Chaitin computers. We shall construct a Chaitin computer C whose sole purpose in making its programs converge is to insure $\Omega \notin W_N$, ~~so~~ for some value of N that C will compute. We turn to the details.

First we need an analog of the recursion theorem. Let $h: \Sigma^* \times \Sigma^* \to \Sigma^*$ be partial recursive. Suppose also that for any y, $h(\cdot, y)$ is a Chaitin computer in its first argument.

Then for some Chaitin computer C,

$$C(x) = h(x, \pi_C).$$

We may deduce this from the usual recursion theorem as follows. Let $s : \Sigma^* \to \Sigma^*$ be such that $s_1(e) = \pi_e$, for e the Gödel number of the Chaitin computer e. ~~By the recursion theorem, we may find C such that~~ Let $s_2 : \Sigma^* \to \Sigma^*$ be such that if e is the number of a Chaitin computer as a partial recursive function, $s_2(e)$ is its Gödel number qua Chaitin computer. By the usual recursion theorem, find C: $C(x) \cong h(x, s_1(s_2(e)))$

where e is a Gödel number for x.

~~We now describe our~~ s:

~~Before begin~~:

We next need a result of Chaitin which we express as follows. Suppose we are given an increasing series of rationals x_n in $[0, 1]$. We imagine receiving the sequence in x_n in real time. Then we can output a ~~seq.~~ prefix free code $\langle s_n \mid n \in \omega \rangle$ which will be generated from the x_n's in an effective fashion so that $\sum 2^{-|s_n|} = x$.

This will follow easily from Chaitin's description of the effective construction of an instantaneous code.

monotone

We easily construct a sequence of dyadic rationals x'_n such that ~~$x'_n \le x_n$~~ $x_n - 2^{-n} \le x'_n \le x_n$.

If $y_0 = x'_0$, $y_{n+1} = x'_{n+1} - x'_n$. And $y_i = m_i/2^{n_i}$, then at stage n, we put in requests à la Chaitin's proof for m_i code words of length n_i. Thus the sum over the constructed code S of $2^{-|s|}$ will be $\sum_{n=0}^{\infty} y_i = \lim_{n\to\infty} x'_n = \lim_{n\to\infty} x_n = x$.

We turn to the construction of C_ℓ. C will first compute the length of its prefix code, and pick $N > 2^\ell$. ~~Now consider Ω, W_N. Since Ω ...,~~ Let $V = W_N$. Note $\mu(W) < 2^{-\ell}$.

C will proceed in stages. At any stage n,

~~Ω is the limit of a sequence~~

C will add a finite of strings. Also at any time n, we will have some finite approximation V_n to V.

Suppose we come to stage n of the definition C. We select a time t_n so large that 1) $t_n > t_{n-1}$ if $n>0$. 2) For any ~~Any~~ strings s added to the domain of C at previous stages, the corresponding string $\pi_c{}^\frown s$ has been computed by U before time t_{n+1}, and so is reflected in the value of $\Omega_{t_{n+1}}$.

Let $\Omega' = \Omega_{t_{n+1}}$, $V' = V_{t_{n+1}}$. If $\Omega' \notin V'$, we do nothing. If $\Omega' \in V'$, let

r be the least real such that $r \notin V'_n$ or $r = 1$. Now ~~as~~ r is rational, since V'_n is a finite union of open intervals with rational endpoints.

We send to our string generating program the request $y_n = (r - \Omega_{s_n}) \cdot 2^{\ell}$. We associate to this request the subset (Ω', r) of V.

Suppose by ~~&~~ inductive hypothesis that

$$(*) \quad \sum_{i=0}^{n-1} y_i \leq 2^{\ell} \mu(V \cap [0, \Omega']). \text{ Then}$$

since

$$2^{\ell} \mu(V) < 1$$

$$1 - \sum_{i=0}^{n-1} y_i \geq 2^{\ell} \mu(V \cap [\Omega', 1])$$

$$\geq y_{n+1}.$$

So $\sum_{i=0}^{n+1} y_i < 1$. Thus we can process the request and insure that by the time step is completed, $\sum \{ 2^{-|s|} : s \in S_{n+1} \} = \sum_{i=0}^{n+1} y_i$.

Thus after time t_{n+1}, $\Omega_{t_{n+1}} \geq \Omega' + 2^{-\ell} y_n$.

So $\Omega^*_{t_{n+1}}$ will be ~~above~~ $\geq r$. This shows that different requests have different subintervals of V associated to them, and shows that $(*)$ continues to hold.

Now suppose that $\Omega \in U_i$ for infinitely many i. Then $\Omega \in V$. Thus ~~Ω~~ for a ~~st~~ for some $a < \Omega < b$, $a, b \in \mathbb{Q}$, $[a,b] \subseteq U$. Pick n so large that $\Omega^*_{t_n} \geq a$, $[a,b] \subseteq V^*_{t_n}$

(Possibly give the proof of $P_3 \rightarrow P_2$ first

Then our construction of C will insure that

$\Omega \geq b$, a contradiction.

I.4 Finally, we give the proof of Theorem I.3:

If x satisfies P_2, then x satisfies P_2.

Let then $\langle U_n \mid n \in \omega \rangle$ be as in the statement of P_2, ~~let~~ ~~be~~ and such that $x \in U_n$ for infinitely many n. We shall show x does not satisfy P_3. We may assume, by deleting finitely many U_i's that $\sum_{i=0}^{\infty} \mu(U_i) < 1$. Let

$$V_n = \{x \mid x \in U_m \text{ for } 2^n \text{ different values of } m\}.$$

Then the V_n's form a decreasing ~~sequence~~

sequence of open sets. In the proof of the previous theorem, we established that the V_n's are simultaneously r.e and that

$$\mu(V_n) \leq 2^{-n}.$$

But $x \in V_n$, all n. Whence x fails to satisfy P_3.

—x—

This last part of I is for my own information and will not appear in Marginalia. I signal pages of preliminary notes not intended for the final ms by a # after the number.

This is proof $P_4 \to P_3$.

Let then $\langle U_n \mid n<\omega\rangle$ be a simultaneously r.e. sequence of open subsets of 2^ω, with $\mu(U_n) < 2^{-n}$. We can effectively associate to U_n, a prefix free code S_n: $x \in U_n \leftrightarrow \exists s \in S_n \; s \subseteq x$. To do this, let $\langle s_i^n \mid i<\omega\rangle$ be a recursive enum of strings : $U_n = \{x \mid s_i^n \subseteq x\}$. We can construct a prefix code $s'_1, \ldots, s'_n, \ldots$: by induction:

$y \geq s_j \leftrightarrow y \geq s'_j$ some $j \leq k$. (This is easy.)

Now apply the Chaitin simulation lemma to get a new code for the s'_i:

$$C(y, t) = s'_{n,i} \quad \text{iff} \quad U(y) = n$$

for some t: $|t| \leq |s'_{n,i}| - n$

$\exists\, C_0$

Thus $x \in U_n \rightarrow \exists\, m$:

$$H(x(m)) \leq m - n + H(n) + C_0$$

(we use here that the U_n's are simult. r.e.)

Now given k, pick n: $n - H(n) - C > k$

(Possible since $H(n) \leq 2\log_2 n$.)

Then $x(m)$ does not satisfy

$x(m) \geq m - k$ all m, since $x \in U_n$.

This completes our reconstruction of Schnorr's

proof that $P_3(x) \Longleftrightarrow P_4(x)$.

The main result of this section is the following theorem.

There is a $C > 0$ such that $\forall n \; \exists$ string s of length n with

$$\tilde{H}(x^* | x) \geq \log n - \log\log n - C.$$

(All log's to base 2)

Here $\tilde{H}(x|y)$ is the length of the shortest program p $\ni$ $U(p, y) = x$.

Note that it suffices to prove the theorem for large n, since we afterwards can adjust C so as to make it true for the finite set of exceptional values. We shall see that any $C > 1$ will work for all sufficiently large n. In what follows, n is always "sufficiently large"

Lemma 1. Let ε sufficiently small.

Let $k = \log n - \log\log n - C$

$$\ell = 2^k + 1$$

$$M = \sum_{0 \le i < \ell} n^{c' i}$$

Then $M < 2^n$, for n sufficiently long

Proof $M \le \dfrac{n^{c'\ell}}{n^{c'} - 1}$

$$\sim n^{c'(\ell-1)}$$

$$\log M \le c' \ell \log n$$

$$\log\log M \le \log\log n + k + \log c'$$

$$\le \log n + [\log c' - C].$$

If $C > \log c'$,
$M < 2^n$.

Our bound in the theorem can be traced back to this lemma.

2. <u>Corollary</u> Suppose that 2^n is divided into l disjoint pieces $A_1, \ldots, A_l$. Then for some i

$$\#(A_i) > n^{c' i}.$$

$$\left(\text{Else } 2^n = \sum \#(A_i) \le M_* \right).$$

Keeping the situation of the corollary, let i minimal $\ni$ $\#(A_i) > n^{c' i}$.

$$\sum_{1 \le j < i} \#(A_j) \le \sum_{1 \le j < i} n^{c' j} =$$

$$\frac{n^{c'(i)} - 1}{n^{c'} - 1} \le n^{c'(i-1)} + O(n^{c'(i$$

Thus for an $\varepsilon' < \varepsilon$, we have:

$$(\exists i) \left(\#(A_i) > n^{2+\varepsilon'} \cdot \sum_{1 \le j < i} \#(A_j) \right)$$

3. We now indicate the particular partition of strings of length n to which we will apply the theorem.

Let $|y| < k$.* We say that y is active for x if

1) $U(y, x)$ is defined (and equals z say)

2) $U(z) = x$.

We assume for the remainder of the proof

1) n is sufficiently large.
2) $\tilde{H}(x^* | x) < k$.

* k as in Lemma 1

It follows that for some p active for x, $U(p, x) = x^*$

There is an analogous notion of p being active for x at time t.

Clearly the number of programs active for x (w.r.t. $|x|$...) is ~~betw~~ between 1 and $2^k - 1$. We let

$A_i = \{ x \mid x$ has $2^k - i$ active programs

(There is an analogous notion of A_i^t:

$A_i^t = \{ x \mid x$ has $2^k - i$ active programs at time $t \}$.

Clearly if $x \in A_i^t$, then if $t' \geq t$, $x \in A_j^{t'}$ for some $j \leq i$.

We apply our corollary and get an i such that if $\bigcup_{j \leq i} A_j = S_i$, then $\#(S_i) \leq 2 n^{(c)(i-1)}$ $+ O(n^{c'(i-1)})$

$\# A_i > n^{(c)i}$

Cost of characters.

1) n $\log n + O(\log\log n)$ bits

2) i : $\leq 2^k$ $k + O(\log k)$ bits

$\log n - \log\log n + O(\log\log n)$ bits.

3) $\#(S_i) \leq n^{C'(i-1)} + O(n^{C'(i-2)})$

$\log \# S_i \leq C'(i-1) \cdot \log n$

$\log\log \# S_i \leq \log i$

$\# S_i$ takes $[C'(i-1) + 1] \log n$ bits

The upshot is that we can describe i, n, & $\# S_i$ in

$(C'(i-1) + 3) \log n + O(\log\log n)$ bits.

Now proceed as follows

1) Wait for all elts of $\bigcup_{j<i} A_j$ to arrive. (This

~~2) When~~

uses # S_i

2) At this point members of A_i are effectively

recognizable, & when x appears, we can compute x^*

Look for the least x. $|x^*| \geq C'(i)(\log n)$.

Such an x must exist.

The description of x we have given takes

$O(1) + C'(i-1) + 3\log n + O(\log\log n)$.

Thus if $C' > 3$, and n is sufficiently large, we have

a contradiction.

[So in write-up, take $C' = 4$, $C = 3$.].

Note that in the current version, the "careful Gödel numbering" is eliminated.

There is a variant of this result, suggested to the author by Chaitin which seems true and which I am unable to obtain by the methods above.

<u>Conjecture</u> There is an infinite sequence x_n of strings so that

1) $|x_n| = n$

2). $H(x_n) \sim n$

3) $\tilde{H}(x^*_n \mid x_n) \sim \log n$

The point is that the x_n's we construct might well satisfy $H(x_n) \leq n / \log \log n$, for example.

III. Relationships between H and K.

Our goal in the following section is to prove the following formulae which relates H and K.

1) $H(x) = K(x) + K(K(x)) + O(K^3(x))$

2) $K(x) = H(x) - H(H(x)) + O(H^3(x))$.

*) $H(x) \asymp K(x \mid H^2(x)) + H^2(x)$

These formulae are really equivalent since we shall also prove:

3) $K^2(x) - H^2(x) = O(H^3(x))$

4) $H^3(x) \sim K^3(x)$

(where the $\sim$ stands for "are asymptotically equal".)

Granted 3) and 4), 1) and 2) are clearly equivalent and give a formula for the number of bits needed to make the optimal Kolmogoroff program self-delimiting, or the cost the optimal Chaitin program pays the we self-deli

Our proof will proceed in three stages. We first get the bound for $H(x)$ in terms of $K(x)$:

5) $H(x) \leq K(x) + H(K(x)) + O(1)$

This is quite easy. ~~Slightly harder is~~ The inequality

6) $K(x) \leq H(x) - H^2(x) + H^3(x) + O(1)$

is more difficult. (Here, e.g., $H^2(x) = H(H(x))$. We shall use a similar notation for iterated logarithms.)

5) and 6) are close to giving 1), the difficulty being that 5) contains HK rather than H^2. However, we can bootstrap our estimate on $K-H$ to get one on $H^2 - HK$ proving 2). At that point 3) and 4) are easy (though somewhat tedious) to obtain, and with them 1).

follows.

Lemma 1 $H(x) \le K(x) + H(K(x)) + O(1)$.

Proof. Let U, V be respectively the universal Chaitin computer and the universal Kolmogoroff computer. Define a Chaitin style computer, C, as follows:

C on input x, first simulates U. Thus if $x = x_1 ^\frown x_2$ with $x_1 \in \mathrm{dom}\, U$, C will compute $U(x_1)$. It then reads exactly $U(x_1)$ further bits of the input, if possible, getting a word x_3, computes $V(x_3)$ and gives it as its output. $\}$

Let y_3 be a minimal Kolmogoroff program for x, and y_1 a minimal Chaitin program for $|y_3|$. Then

$U(\pi_c \frown y_1 \frown y_3) = C(y_1 \frown y_3) = V(y_3) = x.$

Whence $H(x) \le K(x) + H(K(x)) + |\pi_c|$

<u>Lemma 2</u>. Let S_n be the ~~number~~ cardinality of

$\{x : x \in \mathrm{dom}\, U \text{ and } |x| = n\}$.

Then $S_n \le C_2 2^{n - H(n)}$.

<u>Proof</u>. We shall use ~~a~~ Chaitin's lemma for constructing an instaneous code from requests. Each time that we first recognise that $\# S_n \ge 2^k$, we put in a request for a code for n of ~~$\$$~~ length $n-k$ ~~$k=n$~~ $+ 1.2.$

Let n_k be the largest k such that $\# S_n \ge 2^k$.

To be able to cite Chaitin's theorem, we need

7) $$\sum_{n=0}^{\infty} \sum_{0 \le j \le n_k} 2^{-(n-j+2)} \le 1.$$

We now verify this. In the first place,

$$\sum_{0 \le j \le n_k} 2^{-(n-j+2)} \le \sum_{n-n_k+2 \le j < \infty} 2^{-j} \le 2^{n_k - n -}$$

On the other hand,

$$\sum \{ 2^{-|x|} : x \in dom(U) \;\&\; |x| = n \} =$$

$$2^{-n} \cdot \# S_k \;\; \cancel{\le} \ge 2^{-n} \cdot 2^{n_k}.$$

Thus the sum in 7) is less than

$$\sum \{ 2^{-|x|} : x \in dom(U) \} < 1.$$

Let C be the Chaitin computer that implements this code. Let $m = |\pi_C|$. Then

8) $$H(n) \le m + n - n_k + 2,$$

since ~~C(y) = n for some y~~ $U(\pi_c \frown y) = C(y) = n$

for some y of length $n - n_x + 2$. From 8),

$S_x \leq n_x + |A_{\bar{x}}| \leq n - H(n) + (m+3)$,

from which the lemma follows.

<u>Lemma 3.</u> $K(x) \leq H(x) - H^2(x) + H^3(x) + O(1)$

<u>Proof.</u> We ~~go~~ begin by describing a certain Kolmogoroff style computer ~~C.~~ M. ~~C~~ M will depend on a ~~on input x, C first~~ constant C to be fixed presently.

M, on input x, first simulates the universal Chaitin computer U. If U halts on input x, we must have $x = x_1 \frown x_2$ with $x_1 \in \text{domain}(U)$.

7 B computes $U(x_1) = d$, say, and lets $n =$ $|x_2| + d - C$. M next interprets x_2 as a number in the interval $1 \le j \le 2^{|x_2|}$ in the obvious way. Next M proceeds to list the elements of domain(U) of length n in some definite order. (E.g. by the order in which they are computed by U, using lexicographical ordering to resolve ties.) If there are $\geq j$ elements of this set, let y be the j^{th}. (If there are $< j$ elements, M will be undefined at x.) M then outputs $U(y)$.

We claim that one can choose C sufficiently large that for every x, there is a z of length

$H(x) - H^2(x) + H^3(x) + C$ such that

$M(z) = x$. From this the lemma clearly follows.

Let x be given. Let x_1 be the minimal Chaitin program for x. Let x_2 be a minimal Chaitin program for $|x_1| = H(x)$, and let x_3 be a minimal Chaitin program for $|x_2| = H^2(x)$. The z we will construct will have the form $x_3 {}^\frown w$, where $|w| = H(x) - H^2(x) + C$. (So the length of z will be $|w| + |x_3| = |w| + H^3(x)$, as claimed.) To construct such a z, we need to know, with notations as in Lemma 2

a) $S_{H(x)} \leq 2^{H(x) - H^2(x) + C}$.

This is clear from Lemma 2 if we take $C \geq \log_2 C_1$.

~~So we can choose~~ Now M on input $z^\frown w$ will compute the value of n to be $H(x)$. Since a) holds, we can choose w so that x_2 is the w^{th} member of

$$\{y \in \mathrm{dom}\, U : |y| = H(x)\}$$

But then M will evaluate y to be x_2 and will finally output x as its answer. Thus $M(z) = x$, and the lemma is proved.

Lemma 4 $|H(x_1) - H(x_2)| \le H(|x_1 - x_2|) + O(1)$

Proof ~~Given~~ We can construct easily a Chaitin computer that on input y, tries to parse y as $y_1{}^\frown y_2$ with $y_1, y_2 \in \mathrm{dom}(U)$ and then outputs $U(y_1) + U(y_2)$. It follows that

$$H(a+b) \leq H(a) + H(b) + O(1)$$

and similarly if $a \geq b$, $H(a-b) \leq H(a) + H(b) + O(1)$

From this the lemma follows easily.

<u>Lemma 5</u> $H(x) = K(x) + H^2(x) + O(H^3(x))$

We have to see $D(x) = O(H$

<u>Proof</u> Let $D(x) = H(x) - K(x) - H^2(x)$. By Lemmas 1, $D(x) \leq H(K(x)) - H^2(x)) + O(1)$

By Lemma 2, $-H^3(x) \leq D(x)$.

By Lemma 4, $H(K(x)) - H^2(x) \leq$

$H(|K(x) - H(x)|) + O(1)) \leq$

$H(|D(x) + H^2(x)|) + O(1) \leq$

$H(D(x)) + H^3(x)\} + O(1)$.

Putting the results of the first two paragraphs together

we get

10) $|D(x)| \leq H^3(x) + H(|D(x)|) + O(1)$.

I say that from 10) it follows that

) $|D(x)| \leq 2H^3(x)$

for all but finitely many x, whence $D = O(H^3)$, as claimed. (Note that $H(x) \geq 1$, all x else $\phi \in \mathrm{dom}(U)$ & range (U) has 1 element.)

Say $|D(x_n)| \geq 2H^3(x_n)$ where $x_n \to \infty$ as $n \to \infty$. Then $|D(x_n)| \to \infty$ with n whence

$$H(|D(x_n)|) \leq \log(|D(x_n)|) = o(D(|x_n|))$$

Dividing 10) by $|D(x_n)|$, we get

$$1 \leq \frac{H^3(x)}{|D(x_n)|} + \frac{H(|D(x_n)|)}{|D(x_n)|} + O\left(\frac{1}{|D(x_n)|}\right)$$

The last two terms are $o(1)$ and the first has a $\overline{\lim}$ of $1/2$. This is absurd, so we must have

$|D(x)| \leq 2H^3(x)$ for all but finitely many x.

In the following we will need estimates for $Hf(x)$ where $f = O(g)$. We shall use the estimate $Hf(x) = O(\log g(x))$, which is clear since $Hf(x) \leq \log f(x) \leq \log g(x) + O(1)$ (if $f(x) = O(g(x))$.

We have now established 2). Note first that by applying H to both sides of 2), we get

12) $$HK(x) = H^2(x) + O(\cancel{\log}\, H^3(x))$$

Next substitute Kx for x in 2). We get

) $K^2(x) = HK(x) - H^2K(x) + O(H^3K(x))$

Now ~~[illegible]~~ using Lemma 4 on 12), we get

$$H^2K(x) = H^3(x) + O(\log H^3(x)).$$

so $H^2K(x)$ is $O(H^3(x))$. It follows that the two right hand terms in 13) are $O(H^3(x))$.

Thus $K^2(x) = HK(x) + O(H^3(x))$ and from this and 12), 3) follows. Finally ~~fro~~ ~~2)~~, we know $K \sim H$* whence, since $H^2 \to \infty$, $K^3 \sim HK^2$. But ~~from 3)~~, applying H to 3),

$$HK^2 - H^3 = O(\log H^3).$$

Whence $HK^2 \sim H^3$, establishing 4).

* we suppress mention of x.

IV. Relations ~~to~~ between H-randomness and K-randomness of finite sequences.

In this section we study two related questions. First, Kolmogoroff and Chaitin have proposed two related notions of randomness for finite sequences of 0's and 1's, which we will define precisely in a few moments. We prove that every ~~K~~ Chaitin random finite string is Kolmogoroff random but that the converse is false.

The refutation of the ~~cou~~ converse involves a procedure for constructing counterexamples. These also shed light on the question ~~~~ discussed in the preceding section of formulae that compute

$H(x)$ from $K(x)$ or conversely. The formulae of the last section have an error term $O(H^3(x))$. We show in this section that this error term is, in a certain sense, best possible.

Let us recall the notion of Kolmogoroff randomness for finite strings. It is based on two facts:

1) $K(x) \leq |x| + C_0$, for all $x \in \Sigma^*$.

2) $\# \{x : |x| = n \;\&\; K(x) < n + C_0 - j\}\} = O(2^{n-j})$

why not $|x| - \tilde{K}(x \mid |x|)$?

We define $m_K(x) = |x| + C_0 - K(x)$.

Then $0 \leq m_K(x) \leq |x| + C_0$. Roughly speaking, $m_K(x)$ measures the degree of non-randomness of x, and Kolmogoroff random strings are those for which $m_K(x)$

is small.

The analogous facts in the Chaitin context are as follows:

1'): $H(x) \leq |x| + H(|x|) + C_1$

2'): $\# \{ x : |x| = n \;\&\; H(x) \leq n + H(|x|) + C_1 - j \}$

$= O(2^{n-j})$.

why not $|x| - \tilde{H}(x \mid |x|)$

We put $m_H(x) = |x| + H(|x|) + C_1 - H(x)$.

The intuitive interpretation of m_H is similar to that of m_K.

We shall prove

(1) $m_H(x) \geqslant m_K(x) + O(\log_2 m_K(x) + 1)$.

It follows from (1) that if m_H is small

m_K must be small, and this is the sense in which

every Chaitin random real is Kolmogoroff random.

It is easy to prove, using the formulae relating H and K of the last section that

$$m_K(x) \geq m_H(x) + O(\log^2 |x|).$$

Thus if $m_H(x) \gg \log^2|x|$, $m_K(x) > 1$. However, we shall construct an infinite series of strings w_n with the following properties:

a) $|w_n| \to \infty$ as $n \to \infty$.

b) $K(w_n) = |w_n| + O(1)$.

(Thus the w_n's are K-random, for n large.)

c) $\lim\limits_{n \to \infty} \dfrac{m_H(w_n)}{\log^2 |w_n|} = 1.$

It is in this sense that we show that K-randomness

loes not entail H-randomness.

~~Suppose that A is a finite set of integers. The diameter of $A = \max(A) - \min(A)$. If A is empty, diameter $(A) = \phi$.~~

We remark that it would be easy to modify the proof of the preceding section to show

$$\overline{\lim} \quad \frac{H(n) - K(n) - H(H(n))}{H^3(n)} \leq 1.$$

It follows from the example promised in the preceding paragraph that this lim sup is $= 1$.

The same method provides a counterexample to various improvements in the error term of the formulae relating H and K.

Also rules out

$$H(x) = K(x) + H(K(x)) + O(1)$$

We shall prove the following: there are infinite seq. of strings y_n, z_n, w_n:

~~1) $|y_n| = |z_n| = |w_n|$~~

1) $$K(y_n) = K(z_n) + O(1)$$

and $$\lim \frac{H(y_n) - H(z_n)}{\log\log H(y_n)} = -1.$$

2) $$H(y_n) = H(w_n) + O(1)$$

$$\lim \frac{K(y_n) - K(w_n)}{\log\log K(y_n)} = 1.$$

3) $$\lim_{n\to\infty} H(y_n) = \infty.$$

To see how this rules out improvements

in the results of the preceding section, ~~supp~~ we show that the relation

$$H(x) = K(x) + K^2(x) + K^3(x) + O(K^4(x))$$

is false. Indeed, if this were true, since $K(y_n) = K(z_n) + O(1)$, we would have

$$H(y_n) = H(z_n) + O(K^4(y_n))$$

A fortiori,

$$H(y_n) = H(z_n) + O(\log^3 H(y_n)).$$

Hence $\lim \dfrac{H(y_n) - H(z_n)}{\log\log H(y_n)} = 0$,

contrary to our promised example.

We complete ~~this section~~ these introductory remarks by indicating how the example of the K-random ~~reals~~ strings

that are not H-random are concocted. To start with, let ℓ_n be an increasing sequence of integers with $H(\ell_n) = O(\log^{3.5} \ell_n)$. (~~Such a series is easy to construct,~~ (We shall show presently that such a series is easy to construct.) Pick x_n so that 1) $|x_n| = \ell_n$ 2) $\tilde{H}(x_n^* \mid x_n) = \log \ell_n + O(\log\log \ell_n)$. (~~This is~~ The main result of Chapter II guarantees such x_n's.).
Let y_n be the minimal Kolmogoroff program for x_n^* given x_n. Let z_n be a suitably random string of length x_n. Then $w_n = y_n \frown z_n$ will turn out to be K-random, but not H-random.

IV.1 ~~Let us suppose~~ We show now that

$$m_H(x) \geq m_K(x) + O(\log m_K(x) + 1).$$

Indeed, let $L = m_K(x)$.

$$K(x) \cancel{\leq} = |x| + C_1 - L.$$

Thus $H(K(x)) = H(|x|) + O(\log L + 1)$

So $H(x) \leq \cancel{H}\, K(x) + H(K(x)) + O(1)$

$$\leq |x| + H(|x|) + O(1) + O(\log L + 1) - L.$$

So $m_H(x) = L + O(\log L + 1)$

as was to be proved.

IV.2. The following technical lemma will play a key role in our construction of counterexamples:

<u>Lemma</u> $(\forall j)(\exists L)(\forall n)(\forall y)$: If

$K(y \mid n) \cancel{\leq j} \geq |y| - j$, then

$\cancel{\{z \mid y \; K(y^\frown z) \leq\}}$

$\{ z \in {}^n 2 \mid K(y^\frown z) \leq |y| + n - L \}$

has ~~at most~~ less than 2^{n-j} elements.

So, roughly speaking, if y is K-random over n then for many z's of length n, $y^\frown z$ is K-random.

Our proof will proceed by denying the conclusion and then showing that y has a short K-program.

Consider the following special purpose Kolmogoroff computer M.

On inputs x n M first tries to parse x as

$x_1 ^\frown x_2 ^\frown x_3 ^\frown x_4$

where x_1, x_2, x_3 are in dom U. If so, it sets

$$j = U(x_1)$$

$$l = U(x_2)$$

$$m = U(x_3) + |x_4|.$$

M now proceeds to enumerate those y's such that

1) $|y| = m$

2) For at least 2^{n-j} z's,

$$K(y ^\frown z) \leq m + n - L$$

M also ~~converts~~ interprets x_4 as a ~~number~~ positive integer $\leq 2^{|x_4|}$.

and outputs the x_4^{th} such y if it exists.

Let C_0 = sim M.

Now there are at most $2^{n+m-\ell+1}$ pairs (y, z) such that $K(y^\frown z) \le n+m-\ell$. Thus there are at most $2^{m+j-\ell}$ y's which occur in this way with 2^{n-j} z's. Thus if we let x_1, x_2, x_3, x_4 encode respectively j, ℓ, $\ell - j$, and the position of ~~the~~ the same particular y ~~~~ ~~context~~ which has 2^{n-j} z's associated in the list of all such y's, we get a ~~word of length~~ K-program for y of length

$$Sim_M + m - \ell + j + H(\ell) + H(j) + H(\ell - j) \le$$

$$m - \ell + O(j) + O(\log \ell + 1).$$

where the constants in the O's are independent of any n. We now select ℓ so that $\ell \ge j + O(j) + O(\log \ell + 1) + 1$.

Then we get a ~~K~~-program ~~of~~ for y of length $< m-j$. So if $K(y) \geq |y| - j$, ~~with~~ then for the ~~this~~ particular L_a just chosen we must have $< 2^{n-j}$ z's such that $|z| = n$

$$K(y^\frown z) \leq |y| + n - L.$$

IV.4. We now begin our construction of the w_i's which are K-random but not H-random. To start off, let $l_i = 2^{2^{2^i}}$. Then clearly $H(l_i) = H(i) + O(1) = O(\log^3 l_i)$. By the main result of chapter II, select n_i so that

1) $|n_i| = l_i$

2) $\tilde{H}(n_i^* \mid n_i) \geq \log l_i + O(\log^2 l_i)$.

Now by Chaitin's work

$$\tilde{H}(n_i^* | n_i) = \tilde{H}(H(n_i) | n_i) \leq$$

$$\cancel{\log H(n_i) + O(} \; H^2(n_i) + O(1) \leq$$

$$H[\alpha(\ell_i) + H(\ell_i)] = \cancel{\log \ell_i + O(\log^2 \ell_i)}.$$

$$\cancel{H(\ell_i + O(\log^3 \ell_i))} = H(O(\ell_i)) \leq$$

$\log \ell_i + O(\log^2 \ell_i)$. So 2) can be sharpened to read

$$* \; 3) \quad \tilde{H}(n_i^* | n_i) = \log \ell_i + O(\log^2 \ell_i).$$

Let y_i be the minimal K-program for computing n_i^* from n_i. Then $|y_i| = K(n_i^* | n_i)$ $= \tilde{H}(n_i^* | n_i) + O(\log \tilde{H}(n_i^* | n_i))$ by arguments using the relative version of the identity

$$K \leq H + O(1) \leq K + HK + O(1).$$

So $|y_i| = \log l_i + O(\log^2 l_i)$.

Moreover, $K(y_i|n_i) = |y_i| + O(1)$

since y_i is the K-minimal program that computes

n_i^* from n_i.

We now quote the lemma of IV.3 and

get that we can choose z_i so that

1) $|z_i| = n_i$

2) $K(y_i \frown z_i) = \cancel{\log l_i + n_i + O(\log^2} l_i)$

$|y_i| + n_i + O(1)$

3) $H(z_i) = n_i + H(n_i) + O(1)$.

We put $w_i = y_i \frown z_i$.

Then 2) of the preceding paragraph says that w_i is

K-random, and it is evident that $|w_i| \to \infty$ with i.

We next compute $H(|w_i|)$. Indeed

$$H(|w_i|) = H(\cancel{\$}|y_i| + n_i + O(1)) =$$

$$H(n_i) + O(H(|y_i|)) + O(1)$$

But $H(|y_i|) = H(\log l_i + O(\log^2 l_i)) =$

$H(\log l_i) + O(\log^3 l_i) = \cancel{K} \; H(2^i) + O(\log i$

$= O(\log i) = O(\log^3 l_i)$.

Thus $H(|w_i|) = H(n_i) + O(\log^3 l_i)$

Next, we are going to ~~estimate~~ get an upper bound on $H(w_i)$:

$$H(w_i) \le H(w_i | z_i) + H(z_i) + O(1)$$

$$\le H(y_i | z_i) + \overset{H(n_i)}{n_i} + O(1)$$

Now we have $n_i = |z_i|$, so $H(n_i | z_i) = O(1)$.

Also $H(n_i^* | n_i) = O(1)$, so

$$H(n_i^* | z_i) \leq H(n_i^* | n_i) + H(n_i | z_i) + O(1)$$

$= O(1)$.

Now by an easy relativization of a result of Chaitin's, there are $O(1)$ programs of length $|y_i|$ computing n_i^* from n_i.

whence $H(y_i | z_i) \leq$

$H(y_i | n_i^*, n_i) + O(1) \leq$

$H(|y_i| \,|\, n_i^*, n_i) + O(1) \leq$

$\log |y_i| + O(\log \log |y_i|)$

$= \log^2 l_i + O(\log^3 l_i)$.

The upshot is that

$$H(w_i) \leq \cancel{H(n_i)} +$$

$$\log^2 l_i + n_i + H(n_i) + O(\cancel{\ }). \log^3 n_i)$$

So $\cancel{\exists}$ $|w_i| + H(|w_i|) - H(w_i) \geqslant$

$$\cancel{\ } \log l_i + n_i + O(\log^2 l_i) + H(n_i) -$$

$$[O(\log^2 l_i) + n_i + H(n_i)] =$$

$$\log l_i + O(\log^2 l_i).$$

Thus $m_H(w_i) \geqslant \log l_i + O(\log^2 l_i)$

$$\geqslant \log\log n_i + O(\log^3 n_i).$$

$$\geqslant \log\log |w_i| + O(\log^3 |w_i|$$

Which proves the claim ~~that~~ that

$$\overline{\lim} \; \frac{m_H(w_i)}{\log^2 |w_i|} \geqslant 1.$$

As we remarked earlier, it is easy to get a bound on m_H in the other direction, using the methods of proof of III. (In revised version of IV this should be explicitly stated. Also in revised version of I, should state upper bound on $\tilde{H}(n^*_i \mid n_i)$ that follows from Chaitin's work.)

The upshot is:

$$H(w_i) = |w_i| + H(|w_i|) + \cancel{\log}\ Q_i \quad \text{where}$$

$$Q_i \sim \log^2 |w_i|.$$

Now if z_i is H-random of length $|w_i|$, then ~~$~~ since z_i will also be K-random,

$$K(z_i) = |w_i| + O(1), \quad H(z_i) = |w_i| + H(|w_i|) + O(1)$$

This gives z_i with $K(z_i) = \cancel{H(y_i)}\ K(y_i) + O(1)$ &

$$\frac{H(z_i) - H(y_i)}{\log^2 H(y_i)} \longrightarrow 1 \text{ as } i \to \infty.$$

We need a lemma to get v_i say:

$H(v_i) = H(w_i) + O(1)$.

Lemma. Let $n \geq 0$. Then $\exists C$: $\exists m$:

$$| m + H(m) - n | \leq C.$$

Proof. We know

$$| H(x+D) - H(x) | \leq H(D) + C_0.$$

Thus if D is large enough, $D > 2 \log D + C_0 \geq H(D) + C_0$. Fix D. Let now $f(x) = x + H(x)$.

By what we have said, $\cancel{f(D)}$) $f(x+D) > f(x)$.

Also $f(x+D) \le f(x) + 2D$.

Now given m, pick n: $|f(n) - m|$ is minimal.

Then clearly $|f(n) - m| \le 2D$ else one of

$f(n+D)$, $f(n-D)$ would be closer to m.

Now pick u_n: ① u_n is H-random. I.e

1) $H(u_n) = |u_n| + H(|u_n|) + O(1)$

2) $|u_n| + H(|u_n|) = H(w_n) + O(1)$

So of course $H(u_n) = H(w_n) + O(1)$.

Now $K(u_n) = |u_n| + O(1)$.

It remains to compute $|u_n|$.

$- Q_n$

$$|u_n| + H(|u_n|) = |w_n| + H(|w_n|) + |\cancel{\ldots}|.$$

Write $|u_n| = |w_n| + R_n$.

$$H(|u_n|) = H(|w_n|) + O(\log R_n)$$

Thus $R_n + O(\log R_n) \sim \log^2 |w_n|$.

It follows that $R_n \sim \log^2 |w_n|$

Thus ~~$K(|u_n|$~~)

$$K(|w_n|) - K(|u_n|) = R_n \sim \log^2 |w_n|!$$

So all the results claimed in the introduction to this section are now proved.

Caution The result claiming correctness on a set of upper density 1 is not proved, only that it is within $O(1)$ on a set of upper density 1. I should try to figure out what's happening

V. Upper bounds on H.

Let us begin by recalling the following result of Chaitin. Let $f: \omega \to \omega$ be recursive. Then

1) If $\sum_{j=0}^{\infty} 2^{-f(j)} < \infty$,

then

$$H(n) \leq f(n) + O(1), \text{ all } n.$$

2) If $\sum_{j=0}^{\infty} 2^{-f(j)} = \infty$, then

$$H(n) > f(n) \quad \text{for infinitely many } n.$$

In the second case, it is not hard to construct $g: \omega \to \omega$, recursive such that $g(n) - f(n) \to \infty$ as $n \to \infty$ and $\sum_{j=0}^{\infty} 2^{-g(j)} = \infty$. (One can even show that g can be chosen weakly monotone increasing if f is

weakly monotone. Thus the conclusion in 2) is self strengthening to

$$\overline{\lim}\,(H(n) - f(n)) = \infty.$$

This remark also shows that any recursive i.o. lower bound can be infinitely often improved (by replacing f by f + g as above.)

We show that the situation in the upper bound case is quite different. We shall construct a recursive function $h: \omega \to \omega$ such that

1) $h(n) \geq H(n)$ for all n

2) $h(n) = H(n)$ for infinitely many n.

In fact, by an easy argument, 2) can be strengthened to

2*) $\overline{\lim}\ \frac{1}{n} \# \{m: m \leq n \ \& \ h(m) = H(m)\} > 0.$

Our construction of h and our proof of 2) will be quite non-constructive, and in some sense, $\{n \mid h(n) \leq H(n)+c\}$ is quite sparse. We shall prove, in this direction that there is no effective procedure which given n gives a finite set D_n such that a) $m \in D_n \rightarrow m \geq n$ b) $(\exists x \in D_n)\ h(x) \leq H(x)+C$. ~~It follows~~ (Our proof will hold for any recursive upper bound for H.) It will follow easily that

$$\underline{\lim}\ \frac{1}{n} \# \{m: m \leq n \ \& \ h(n) \leq H(m)+C\} =$$

The basic idea behind our construction of h is to choose f so that $\sum^{\infty} 2^{-f(j)}$ converges "as slowly" as possible

One byproduct is the construction of an recursive convergent sequence of positive reals $\langle a_n \mid n < \omega \rangle$ $\ni$ if $\langle b_n \mid n < \omega \rangle$ is any recursive convergent sequence of positive reals, then

$$\overline{\lim} \frac{a_i}{b_i} > 0.$$

We remark that with a little extra work we can arrange that f be monotone increasing. We sketch this modification without giving complete details.

V. 1. We begin by giving the construction of the slowest growing convergent sequence, a_n. (Since there is no sort of uniqueness proved, we should really say ~~minimally slow growing~~ "minimally growing" but we permit ~~ourselves~~ ourselves to be sloppy.)

Let us recursively enumerate all pairs consisting of

1) a partial ~~function~~ recursive function mapping ω into the positive rationals, h.

2) ~~A positive rational s:~~

2) $1 > \sum_{i \in \mathrm{dom}(h)} h(i)$

Such an enumeration is easy to construct by ~~[illegible]~~ taking ~~pairs s satisfying only 1), 2)~~ the standard enumeration ~~of partial recursive functions~~ of partial recursive functions T and shutting off the partial recursive function if it is about to violate 2)

We define a recursive function $a: \omega \to Q^+$ as follows: Case 1 $n = 2^i 3^j 5^k$, $h_i(j)$ ~~[illegible]~~

is ~~first~~ computed in exactly k steps. Then

$$a_n = 2^{-(i+2)} \cdot h_i(j).$$

(5) Case 2. Otherwise Say Case 2 is occuring at stage n for the m^{th} time. Put

$$a_n = 2^{-(m+1)}.$$

We claim first $\sum a_n < 1$.

Indeed Case 2 contributes at most $1/2$ to the sum. Numbers of the form $2^i 3^j 5^k$ for each fixed i contribute at most

$$2^{-i-2} \cdot \sum_{j \in dom(h_i)} h_i(j) < 2^{-i-2}.$$

Thus Case 1 contributes at ~~most~~ less than $1/4 + 1/8 + \cdots = 1/2$ to the sum. So $\sum^{\infty} a_n < 1$

Suppose $\langle b_i : i \in \omega \rangle$ is recursive and $\sum b_i < \cancel{1}\,\infty$.

~~By scaling~~ Pick $\lambda \in \mathbb{Q}$: $\sum_i \lambda b_i < 1$.

Now ~~$\lim_i b_i/a_i$~~ $\overline{\lim} \frac{\lambda b_i}{a_i} = \lambda \overline{\lim}\, b_i/a_i$.

Thus, without loss of generality, we may assume

$\sum_i \cancel{\lambda} b_i < 1$.

So $b_i = h_n(i)$ for some fixed n.

If $\overline{\lim}$ ~~b_i/a_i~~ $a_i/b_i = 0$,

then $a_i < 2^{-(n+3)} b_i$ for i ~~larger than i_0~~ $\geq i_0$, say.

We now define an infinite series c_n:

$c_{n+1} = \cancel{2^{k_n} 3}\ 2^n 3^{k_n} 5^{j_n}$

where $h_n(k_n)$ is computed in exactly j_n steps.

By construction $a_{i_{n+1}} = 2^{-n-2} b_{i_n}$.

$$b_{i_{n+1}} \geq 2^{(n+3)} a_{i_{n+1}} \geq 2 \cdot b_{i_n}.$$

But then $\sum_{n=0}^{\infty} b_{i_n}$ diverges exponentially contradicting our assumption that $\sum_i b_i$ is convergent.

V. 2. Our construction of f will be similar to that of the a_i's. Again f at various stages will be imitating H at earlier stages, and if H too closely imitated f, we would get $\sum 2^{-H(n)} = \infty$, contrary to fact.

Let $\langle i_n, j_n \rangle$ be a recursive enumeration without [illegible] repetitions of all pairs $\langle i, j \rangle : j \geq H(i)$ so that $i_n < n$. ~~At~~ Let

step $g(n) = j_n + 2$

We claim first $\sum_{j=0}^{\infty} 2^{-g(n)} < 1$. Indeed

$$\sum_{j=0}^{\infty} 2^{-g(n)} = \sum_{i=0}^{\infty} \sum_{j \geq H(i)} 2^{-j-2} =$$

$$\sum_{i=0}^{\infty} 2^{-H(i)-1} \leq 1/2 < 1.$$

It follows that $g(n) \geq H(n) - C$ for some positive C, by the result of Chaitin recalled at the start of this section.

I say that $g(n) < H(n) + 3$ for infinitely many n. Suppose to the contrary that $g(n) \geq H(n) + 3$ for $n \geq k_0 > 0$. Define an infinite series of integers k_n, j_n as follows

$j_n = H(k_n)$;

k_{n+1} is the stage at which $\langle k_n, j_n \rangle$ is listed.

Then $k_n < k_{n+1}$ &

& $g(k_{n+1}) = H(k_n) + 2$.

Thus $H(k_{n+1}) \leq g(k_{n+1}) - 3 \leq H(k_n) - 1$.

So $H(k_n)$ is an infinite decreasing sequence of non-negative integers, and we have reached an absurdity.

Thus $H(n) \leq g(n) + C$ for all n,

but $H(n) > g(n) - 3$ for infinitely many n.

Pick C' minimal in $\mathbb{Z}$ such that $H(n) \leq g(n) + C'$ for infinitely many n

(So $-2 \leq C'$.). Evidently,

$H(n) = g(n) + C'$ for infinitely many n. (Else

C' could be replaced by $C' - 1$.). Now put $h(n) =$ $g(n) + C'$. Then $h : \omega \to \omega$ is recursive and satisfies 1) & 2) of the introduction.

(If we desired to get h monotone, we would construct a monotone g and arrange to assign to each pair $\langle i, j \rangle$ a block $B_{i,j}$ so that

① $$\sum_{n \in B_{i,j}} 2^{-g(n)} = 2^{-j-2}.$$

② The $B_{i,j}$'s are pairwise disjoint & $i < \min(B_{i,j})$.

We would then construct assuming $H(n) \leq g(n) - 3$, an infinite series of blocks S_i :

$$\sum_{s \in S_{i+1}} 2^{-H(s)} \geq 2 \left(\sum_{s \in S_i} 2^{-H(s)} \right)$$

which would contradict $\sum_s 2^{-H(s)} < 1$.

his / tion / ow / ms / , / ror!!

V. 3. Recall from Chaitin's work that $\exists\, C_0$:

1) $H(n) \leq H(\lfloor \log n \rfloor) + C_0$, all n

2) $H(n) \geq H(\cancel{\log n}\ m) - C_0$, ~~i.e.~~ for at least ½ the n's with $\log n = m$

Thus if we let $h_1(n) = h(\lfloor \log n \rfloor) + C_0$,

then by 1), $h_1(n) \geq H(n)$.

Also if ~~h(log~~ $h(m) = H(m)$, then

$h_1(n) \leq \cancel{H(\ )} \leq H(n) + 2C_0$, for at least

~~Thus for some j with 0 ≤~~

½ of the n's in $[2^{m}, 2^{m+1})$, and thus for at least

½ ... $[2^m, 2^{m+1})$

Thus for some j and infinitely many m,

$$\{ n < 2^{m+1} : h_1(n) = H(m) + j \} \geq 1/8c_0 \cdot 2^m$$

This establishes 2*) with h replaced by h_1.

(We may clearly arrange that 2) holds as well ~~by~~ by replacing h^* if necessary by $h^* - C$.

V.4. We now let $h : \omega \to \omega$ be an arbitrary recursive upperbound for H. We shall assume that we have an effective procedure that assigns to each n a ~~it~~ finite set D_n so that 1) $\min D_n > n$

2) $\exists x \in D_n : h(x) - C \leq H(x)$.

We shall proceed to derive a contradiction.

First, we define an infinite ~~series~~ recursive sequence E_i of finite sets by putting $E_0 = D_0$,

$E_{n+1} = D_{m_n}$ where $m_n = \max(E_n)$.

Thus, in addition to 2), the E_n's satisfy

3) $i < j \to E_i \cap E_j = \emptyset$.

Let $\gamma_n = \sum_{j \in E_n} 2^{-f(j)}$.

Now $\sum_j 2^{-f(j)} \leq \sum_j 2^{-H(j)} < 1$.

So 3) entails $\lim_{n \to \infty} \gamma_n = 0$.

We now define a ~~[illegible]~~ Chaitin machine M

that runs as follows:

1) M searches untill it finds an n such that

$-\log_2 \gamma_n \geq \sin M + C + 1.$

(Note that by a standard use of the recursion theorem, M may be allowed to know its simulation cost. Since f, $E_\bullet$ are recursive, so is γ_n. Since $\gamma_n \to 0$ as $n \to \infty$, M's search will succeed.

2) M now constructs an ~~instance~~ instantaneous code for E_n so that the code word for x has length $A(x) - \sin M - C - 1$.

(This is possible by (*) & Chaitin's theorem ~~Even is finite by using the Huffman code~~.)

3) M now examines its input y. If y is one of the

code words of S, then M outputs the corresponding element of E_n.

It follows that for $x \in E_n$,

$$H(x) \leq h(x) - A - 1,$$

~~contrary~~ contrary to our assumption 2).

Now, if

$$\overline{\lim}\ 1/n \# \{ m < n : h(m) - A \leq H(m) \} > c,$$

then we could take $D_n = [n, \lambda n]$ where λ is chosen so that $\frac{n-1}{\lambda n} < c$, contrary to the theorem just proved. Thus all claims made in the introduction to this section have been established.

Aug. 15, 1979

Enclosed is a ~~prelim~~ revised version of Chapter II. I should note that precisely this result was published in a Russian journal (by Gac, I believe). Offhand, I don't know the reference; Greg Chaitin, (IBM Wat. Labs), probably would have it.

Some background to put the result in perspective (See also the remark at the end of this letter.) Let $\phi(n) = \sup \{ \tilde{H}(x^* | x) : |x| = n \}$. Chaitin had previously shown that $\phi(n) \to \infty$, as $n \to \infty$. His proof was non-constructive, and did not get a recurs lower bound tending to ∞.

It is not hard to show $\tilde{H}(x^* | x) \leq \log n + \log\log n + O(\log\log\log n)$ (if $|x| = n$). (Th our lower bound is fairly sharp.) In fact let $w =$

but finitely many n.

C and C_1 will be rationals.

Let C_1 be chosen with $2 < C_1$; $\log C_1 < C$

Let $k = \lfloor \log n - \log\log n - C \rfloor$. Let $\ell = 2^k$.

Let $M = \sum_{1 \le i \le \ell} n^{c' \cdot i}$. Then $M \le 2^n - 1$, for all sufficiently large n.

Hence if the set of strings of length n is partitioned into ℓ pieces, then for some $i \le \ell$, $\#(A_i) \geq$

If i is least such, then

$$\#\left(\bigcup_{j<i} A_j\right) \le \sum_{1 \le j < i} n^{c' \cdot j}$$

$$\le 2 \cdot n^{c'(i-1)} \qquad \text{(for } n \text{ sufficiently large.)}$$

~~Hence, if we pick $\varepsilon > 0$ sufficiently small,~~

~~then~~

$$\cancel{(1) \qquad n^{2+\varepsilon} \cdot \#\left(\bigcup_{j<i} A_j\right) < \#(A_i).}$$

Next I wish to describe the particular partition of strings of length n that I will apply these remarks to. Let x be a string of length n. By our assumption that $\tilde{H}(x^* | x) < k$, for some p with $|p| < k$, we have $U(p | x) = x^*$; $U(x^*) = x$.

<u>Definition</u>. Let $|x| = n$, $|y| \le k-1$. Then y is active for x if $U(y|x)$ is defined ($\exists\, z$ s and $U(z) = x$.

Let $1 \le j \le 2^k$. Then $A_j =$

$\{x$: There are precisely $2^k - j$ programs active for $x\}$

At a given stage t, we can define an analogous notion of active for x at stage t, and get a corresponding ~~notion~~ partition A_j^t. Note that $x \in A$ implies that for all $s \ge t$, $x \in A_i^s$ for some i

Also $A_{2^k} = \emptyset$ since x^* gives rise (as remarked earlier) to at least one program active for x.

Let i be least such that $\#(A_i) > n^{c' \cdot i}$.

We code finite sequences of integers into integers in some standard way. $\langle\langle x_0, \ldots, x_{n-1} \rangle\rangle$ is the seq. no. of the sequence $\langle x_0, \ldots, x_{n-1} \rangle$. Let $S_i = \bigcup_{j<i} A_j$

<u>Lemma</u>. $H(\langle\langle n, i, \#(S_i) \rangle\rangle \leq$

$[C'(i-1) + 2] \cdot \log n + O(\log \log n)$.

<u>Proof</u> 1. $H(n) \leq \log n + O(\log \log n)$

2) $H(\langle\langle n, i \rangle\rangle) \leq$ $\cancel{H(n) + H(i|n) \leq}$

$H(n) + \tilde{H}(i|n) + O(1)$.

(Recall: $H(x|y) = \min z: \; U(z|y^*) = x$;

$\tilde{H}(x|y) = \min z \quad U(z|y) = x$)

$$\tilde{H}(i|n) \le \tilde{H}(i|k) + \tilde{H}(k|n) + O(1)$$

Since clearly $\tilde{H}(k|n) = O(1)$, $\tilde{H}(i|n) \le \tilde{H}(i|k)$

3) Since $i \le 2^k$, clearly $\tilde{H}(i|k) \le k + O($

So $H(\langle\langle n, i\rangle\rangle) \le 2\log n + O(\log\log n)$

4) By previous remarks,

$$\#S_i \le 2 \cdot n^{c' \cdot (i-1)}$$

Thus $H(\langle\langle n, i, \#S_i\rangle\rangle) \le$

$$\tilde{H}(\#S_i \mid \langle\langle n, i\rangle\rangle) + H(\langle\langle n, i\rangle\rangle) + O(1)$$

$$\le \tilde{H}(\#S_i \mid 2 \cdot n^{c'(i-1)}) + \tilde{H}(2 \cdot n^{c'(i-1)} \mid \langle\langle n$$

$$+ H(\langle\langle n, i\rangle\rangle)$$

$$\le c' \cdot (i-1) \cdot \log n + 1 + O(1) +$$

$$2\log n + O(\log\log n) + O(1)$$ q.e.d. Lemma

The remainder of the arguement can be summarized as follows. We will describe a uniform recursive procedure Ψ with the following property. Suppose 1) n is sufficiently large, 2) $\phi(n) < k$. Then $\Psi(\langle\langle n, i, \# S_i\rangle\rangle)$ will be a string of length n, x, such that $H(x) \geq \lfloor C' \cdot i \cdot \log n \rfloor$.

On the other hand, $H(x) \leq H(\langle\langle n, i, \# S_i\rangle\rangle) + O(1) \leq [C' \cdot (i-1) + 2] \log n + O(\log \log n)$. This gives a contradiction for n sufficiently large.

Here is our description of Ψ:

1) Wait for a time t_0 so large that a) $A_{2k}^{t_0} = \emptyset$; b) $\# S_i^{t_0} = \# S_i$. (Recall that Ψ is given as input the parameters $n, i, \# S_i$.)

At any time $t > t_0$, $S_i^t \supseteq S_i^{t_0}$ (recall that numbers tend to migrate downward in our partition). Since $S_i^{t_0} \subseteq S_i^t \subseteq S_i$ & $\# S_i^{t_0} = \# S_i$, we have

$S_i^{t_0} = S_i^t = S_i$.

2) Hence if $x \in A_i^t$ for some $t \geq t_0$, then $x \in A_i$. (For otherwise, $x \in S_i$, $x \notin S_i^t$, contradicting 1) $t \geq t_0$.

3) Suppose $x \in A_i^t$, Then we can compute x^* by the following procedure. Let $y_1, \ldots, y_m$ be all those strings active for x at time t. Since $x \in A_i$, these are the only strings ever active for x. Let $z_i = U(y$

Then since $\phi(n) < k$, some $z_i = x^*$. Since $U(\cancel{x^*} z_i) = x$, all i, x^* is the least z_i. Hence for $x \in A_i^t$, $t \geq t_0$, we can effectively compute $H(x)$ (from the data x, n, i, $\# S_i$).

~~4) Since $\# A_i \geq n$~~

4) Since $\# A_i > n^{c' \cdot i}$, some $x \in A_i$ has $H(x) \geq \lfloor c' \cdot i \cdot \log n \rfloor$. Let $\langle x_1, t_1 \rangle$ be the least pair $\ni$ 1) $t_1 \geq t_0$

2) $x_1 \in A_i^{t_1}$

3) $H(x_1) \geq \lfloor c' \cdot i \cdot \log n \rfloor$

Then x_1 is the output of the procedure ψ.

As indicated earlier, this completes the proof.

Note that $\tilde{H}(x^* | x)$ is of interest in the Chaitin theory as "the difference" between the more conceptual ~~$\tilde{H}(x|y)$~~ $\tilde{H}(y|x)$ and the correct $H(y|x)$ ($= \tilde{H}(y|x^*)$). I.e. the identity

$$H(\langle\langle x, y\rangle\rangle) = H(x) + H(y|x) + O(1)$$

would not be valid with $H(y|x)$ replaced by $\tilde{H}(y|x)$ (and in the case $y = x^*$ would be off by the term $\tilde{H}(x^*|x)$.)

As ever,

Bob.